A Project Report

On

Comparative Analysis of Credit Card Fraud Detection using Machine Learning and Deep Learning Techniques

Submitted by

Anjali Chouhan

(Roll No. 2301101001)

Submitted to

Dr. Aruna Tiwari

(Professor)

For the fulfillment of

CS 403/603: Machine Learning — Autumn 2023

Department of Computer Science & Engineering,
Indian Institute of Technology Indore
MP, India

Contents

Chapter 1

Introduction

Banking fraud is defined as the unauthorized use of an individual's confidential information to make purchases, or to take away funds from the user's account. The use of online shopping, digital payments, net banking, and transactions through payment cards is increasing day by day. Fraud detection system should distinguish between fraud transactions and normal transactions and make the detection possible in real-time transactions. Credit card fraud increases daily and fraudsters' actions rarely follow one predictable pattern. [1].

E-banking popularity is increasing rapidly, which results in increasing online transactions owing to heavy online shopping and immediate online bill payment. Consequently, the fraud cases have also increased, putting great burdens on the economy and affecting both customers and financial institutions [2]. Moreover, fixing the harm done is a money consuming and time-consuming task. It is difficult to build an efficient fraud detection and prevention system that works in real-time, as the number of fraudulent card transactions is very small compared to the total volume (VISA alone processes over 65,000+ transactions every second). Hence, establishing a training set is difficult due to the highly unbalanced data [3].

Traditional rule-based systems are insufficient, often resulting in false positive rates that exceed 90%. Further, this gives rise to a huge number of false positive alerts that need to be manually cleared by human intervention. Repetitive analyst action can lead to a significant number of "false positives", raising the operational risk and subsequently regulatory risk in the process. Merchants, Acquirers, and Issuers have started to create solutions to bring down fraud transactions to a minimum and decrease merchant chargeback rates. The longtime delay between fraud transaction time and the time taken to detect it is one of the main challenges of fraud prevention. This means that if there is no fraud prevention technique, fraudsters can easily inflict huge damage on a business before any stakeholder realizes the problem [4].

According to Shift Processing article on credit card theft statistics in 2018, $24.26 billion was lost due to the payment card frauds committed worldwide. The USA alone suffered 38.6% of reported card fraud losses in 2018. Credit card fraud increased by 18.4% in 2018 and it is on the rise. Card-Not-Present (CNP) fraud is now 81% of the cases, more than Point-of-Sale (POS) fraud. Identity theft was the 3rd largest cause of fraud in the USA in 2018, 14.8% of the reported frauds. Credit card fraud was on top of the list of Identity theft fraud. In 2018, credit card fraud was almost 35% of all identity theft frauds. Yahoo's breach in 2013 resulted in the exposure of 3 billion victims, the biggest single informational breach. Also, in 2018, the data breaches in

Business Sector were 46%, including the Marriott data breach. 69% of frauds started with a consumer being contacted by telephone or email, for overdue loans or prize scams, for example. Moreover, the report focused on the top 7 data breaches of all Time: (1) Due to Yahoo data breach in 2013, 3 billion consumers in total were exposed. It is considered the biggest single data breach; (2) First American Financial Corp. had 900 million customer files exposed in 2019; (3) 540 million users' information was exposed by Facebook in 2019; (4) The biggest breach was by Marriott International in 2018 which exposed as many as 500 million records; (5) Adult Friend Finder had 412 million records compromised in 2016; (6) Equifax had 143 million records exposed in 2017, and (7) In 2019, Capital One had more than 100 million records which could have been exposed [5].

1.1 Motivation of the project

The major objective of this report is to do a comparative study of prevalent and some unexplored machine learning and deep learning algorithms in identifying fraudulent credit card transactions. Credit cards offer an effective and user-friendly function, so people can use them for online transactions. Utilization of credit cards has increased, and with that, so has the potential for credit card fraud. Financial institutions as well as cardholders suffer considerable financial losses as a result of credit card theft. The recent development of Deep learning algorithms has been the key area of concentration in this regard. To get effective results, a comparative study on Deep Learning and Machine Learning algorithms was conducted.

1.2 Objective of the project

The objective of this report is to comprehensively investigate and elucidate the dynamics of credit card fraud detection, with a specific focus on the knn, random forest, svm, CNN & gan algorithms. Through an in-depth exploration of these methodologies, the report aims to:

1. Provide a clear understanding of the role of machine learning approaches knn, random forest and svm in detection of credit card fraudulent transaction.

2. Examine the impact of deep learning CNN and gan on credit card fraud detection, elucidating how neural networks extract intricate patterns and latent features to enhance prediction accuracy.

3. Explore the comparative synergy between machine learning and deep learning, showcasing how their combined strengths create a more nuanced and effective approach to credit card fraud detection.

4. Highlight the significance of credit card fraud detection in the context of contemporary world technological advancement, and the evolving landscape of digital financial transactions.

1.3 Contribution of the project

The contributions of this report are as follows:

1. Safety in credit card usage: Understanding credit card fraud detection with Machine Learning (ML) and Deep Learning (DL) empowers users & the financial world to have safety regarding the use of credit cards, appreciating the technology behind fraud detection and enhancing their overall usage experiences.

2. Inspiration for Innovation: The report serves as inspiration for industry professionals, sparking innovation in credit card fraud detection by highlighting the impact of ML and DL and encouraging further exploration for refining algorithms and creating more accurate, exact fraud detection and avoidance.

1.4 Organization of the report

The introduction of this report is provided in Section.1 mentioning the applications, challenges, problems and solutions in credit card fraud detection followed by the motivation and objective of the thesis. Section 2 discusses the background and literature survey of our research in detail. Section 3 highlights the methods of our project work and experiments. Finally, Section 4 concludes the report.

Chapter 2

Literature Review

In this chapter, we present a brief overview of the literature related to credit card fraud detection. Kaithekuzhical Leena Kurien et al. [6], proposed that machine learning methods work well in detecting fraudulent transactions because they have high computing capacity and the ability to handle enormous datasets. With machine and deep learning, a number of real-world issues can be predicted, including email spam, fraud detection, and medical diagnostics. The fact that credit card passwords, CVV numbers, and other crucial data are always vulnerable due to the extensive use of e-commerce and online purchasing was one of the project's biggest setbacks.

Machine learning techniques, which model the statistical features of transactions, can greatly reduce the reliance on expert experience. The commonly used machine learning methods mainly include SVM [7], [8], KNN [9], [10], and HMM [11], [12]. In addition, ensemble models such as Random Forest and AdaBoost are often employed to improve detection accuracy [13], [14]. However, traditional machine learning methods cannot model the complex spatio-temporal dependencies of user transaction sequences.

Najadat et al. [15], is based on implementation of a model for credit card fraud detection model based on LSTM, GRU. The results of this model were compared against some machine learning classifiers such as Naïve Bayes, ELM, KNN, SVM and the observations were compared and it was that the model based on LSTM and GRU was outperforming the others.

Zhou et al. [[16], used a graph embedding algorithm on their data set, to form relationship network graph which connected different entities together according to relationships, to analyze from relationship perspective. The graph algorithms were able to characterize high risk features in fraud, such as batch attacks, third-party participation etc. Which proved to be more effective in identifying abnormal group frauds. It was discovered that Precision rates were higher in Node2Vec compared to SVM.

Recently, deep learning neural networks have been widely used in credit card fraud detection due to their superior performance in extracting spatio-temporal features. Convolutional Neural Networks (CNN) are often applied to automatically extract features and construct supervised classifiers [17], [18]. Recurrent Neural Networks (RNN) are often used to extract the temporal dependencies within user transaction sequences [19], [20]. However, these models require a large number of fraud transactions for training, so they are not suitable for scenarios with few fraud transaction training samples.

In this work, We propose a significant innovation the use of Generative Adversarial Networks (GANs) to generate synthetic samples of the minority class (fraudulent transactions) to address the issue of imbalanced datasets. This is achieved through a combination of a generator network, which creates synthetic data, and a discriminator network, which distinguishes between real and synthetic data. The generator and discriminator networks are trained simultaneously in an adversarial fashion. Additionally, the work introduces the concept of class weights to balance the difference in occurrences of class labels during training. This is crucial for handling imbalanced datasets, where fraudulent transactions are often significantly outnumbered by legitimate ones. The weighted cross-entropy loss function is used to assign different weights to the classes, emphasizing the importance of correctly classifying fraudulent transactions. Furthermore, we implement random under-sampling using the imbalanced-learn library to address the class imbalance issue in the training data. This technique helps to create a more balanced distribution of classes, enhancing the model's ability to learn from both normal and fraudulent transactions.

CNNs are traditionally used in image processing, but in this work, we apply them to the one-dimensional structure of credit card transaction data. The work explores the impact of different CNN architectures by varying the number of convolutional layers, batch normalization, and dropout layers, providing a comprehensive analysis of their effects on model performance. Moreover, the work introduces the concept of max-pooling layers, which are used to reduce the dimensions of feature maps. This technique helps in reducing the number of parameters to learn, thus addressing overfitting and improving computational efficiency.

Unlike some previous research that may not explicitly handle imbalanced datasets, this work takes a proactive step by visualizing and acknowledging the class imbalance issue.

We also compare the results of the techniques of Random Forest, KNN, SVM, CNN, & GANs.

Chapter 3

Experiment

In this chapter, we discuss the dataset and its preprocessing, various ML & DL methods, and the credit card fraud detection Machine learning and deep learning approaches.

3.1 Dataset specification

The dataset contains transactions made by credit cards in September 2013 by European cardholders.

This dataset presents transactions that occurred in two days, where we have 492 frauds out of 284,807 transactions. The dataset is highly unbalanced, the positive class (frauds) account for 0.172% of all transactions.

It contains only numerical input variables which are the result of a PCA transformation. Unfortunately, due to confidentiality issues, we cannot provide the original features and more background information about the data. Features V1, V2, … V28 are the principal components obtained with PCA, the only features which have not been transformed with PCA are 'Time' and 'Amount'. Feature 'Time' contains the seconds elapsed between each transaction and the first transaction in the dataset. The feature 'Amount' is the transaction Amount, this feature can be used for example-dependant cost-sensitive learning. Feature 'Class' is the response variable and it takes value 1 in case of fraud and 0 otherwise [21].

The dataset and its specifications are discussed in Table 3.1 3.2 3.3.

Dataset shape	(284807, 31)
Fraud Cases	492
Normal Transactions	284315
Minimum rating	0.0
Maximum rating	25691.16

Table 3.1: Normal Dataset specifications

3.1.1 Extract dataset

The process of extracting the dataset for our Credit Card Fraud Detection System project was a critical initial step in developing a robust and effective model. The collected dataset encompasses a significant volume of information, including details on amount,

Dataset shape	(492, 31)
count	284315.000000
mean	88.291022
std	250.105092
min	0.000000
25%	5.650000
50%	22.000000
75%	77.050000
max	25691.160000

Table 3.2: Fraud Dataset specifications

Dataset shape	(284315, 31)
count	492.000000
mean	122.211321
std	256.683288
min	0.000000
25%	1.000000
50%	9.250000
75%	105.890000
max	2125.870000

Table 3.3: Dataset specifications

timelapse, and their parameters.

Splitting Data into Train and Validation Set:-

In the process of comparative analysis of Credit Card Fraud Detection System using Machine Learning and Deep Learning Techniques, the dataset was split into training and validation sets. This step is crucial for training and evaluating the model effectively. The training set, constituting a majority of the data, was used to train the detection model, while the validation set, representing a smaller portion, served to assess the model's performance and generalization to new data. This split allows for an unbiased evaluation of the model's effectiveness before applying it to unseen data, contributing to the overall robustness and reliability of the detection system.

Visualizing the Dataset:-

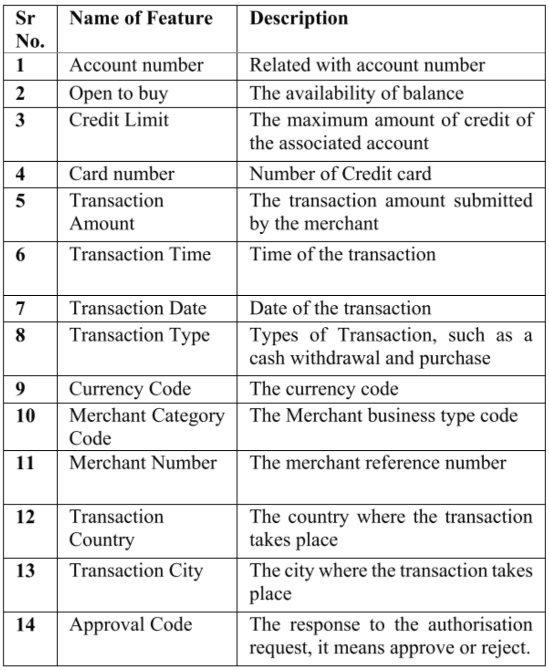
3.1 specifies the raw credit card data that can be extracted from the credit card transactions.

3.2 specifies the pca transformed credit card data that is used for the evaluation of algorithms.

3.3 reads and display the pca transformed credit card data that is used for the evaluation of algorithms.

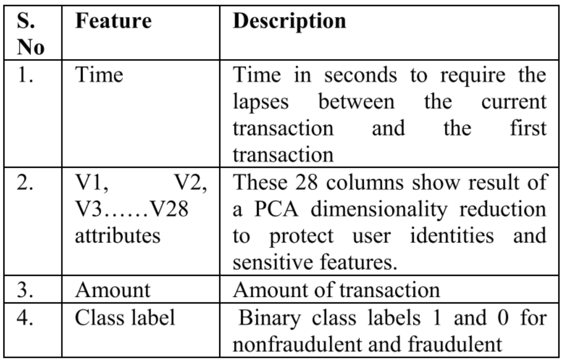
3.4 displays the fraud and normal cases counts of the pca transformed credit card data

3.5 displays Amounts of transaction by class of the pca transformed credit card data
3.6 displays Histogram of Numerical columns of the pca transformed credit card data



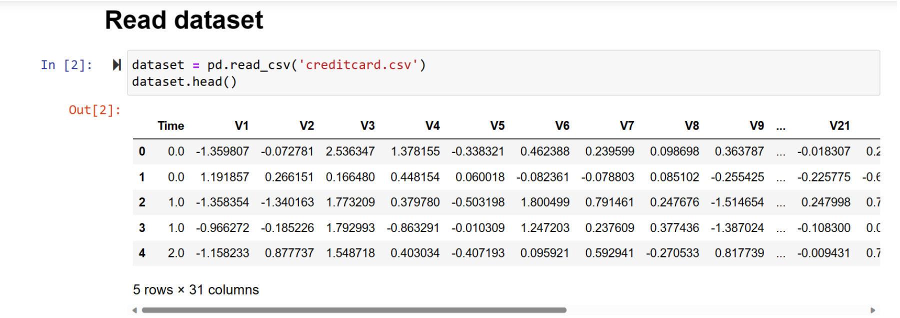
Sr No.	Name of Feature	Description
1	Account number	Related with account number
2	Open to buy	The availability of balance
3	Credit Limit	The maximum amount of credit of the associated account
4	Card number	Number of Credit card
5	Transaction Amount	The transaction amount submitted by the merchant
6	Transaction Time	Time of the transaction
7	Transaction Date	Date of the transaction
8	Transaction Type	Types of Transaction, such as a cash withdrawal and purchase
9	Currency Code	The currency code
10	Merchant Category Code	The Merchant business type code
11	Merchant Number	The merchant reference number
12	Transaction Country	The country where the transaction takes place
13	Transaction City	The city where the transaction takes place
14	Approval Code	The response to the authorisation request, it means approve or reject.

Figure 3.1: Credit Card Data



S. No	Feature	Description
1.	Time	Time in seconds to require the lapses between the current transaction and the first transaction
2.	V1, V2, V3……V28 attributes	These 28 columns show result of a PCA dimensionality reduction to protect user identities and sensitive features.
3.	Amount	Amount of transaction
4.	Class label	Binary class labels 1 and 0 for nonfraudulent and fraudulent

Figure 3.2: Credit Card PCA Data



Read dataset

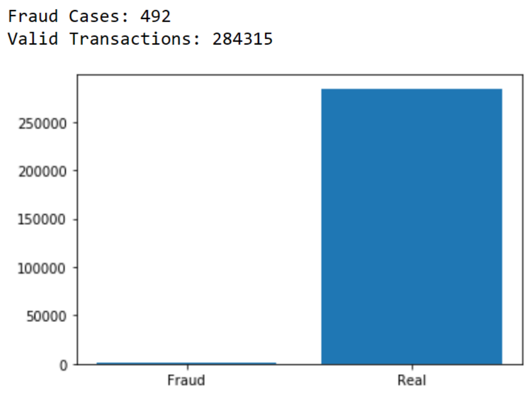
In [2]:
```
dataset = pd.read_csv('creditcard.csv')
dataset.head()
```

Out[2]:

	Time	V1	V2	V3	V4	V5	V6	V7	V8	V9	...	V21	
0	0.0	-1.359807	-0.072781	2.536347	1.378155	-0.338321	0.462388	0.239599	0.098698	0.363787	...	-0.018307	0.2
1	0.0	1.191857	0.266151	0.166480	0.448154	0.060018	-0.082361	-0.078803	0.085102	-0.255425	...	-0.225775	-0.6
2	1.0	-1.358354	-1.340163	1.773209	0.379780	-0.503198	1.800499	0.791461	0.247676	-1.514654	...	0.247998	0.7
3	1.0	-0.966272	-0.185226	1.792993	-0.863291	-0.010309	1.247203	0.237609	0.377436	-1.387024	...	-0.108300	0.0
4	2.0	-1.158233	0.877737	1.548718	0.403034	-0.407193	0.095921	0.592941	-0.270533	0.817739	...	-0.009431	0.7

5 rows × 31 columns

Figure 3.3: read and display Credit Card PCA Data



```
Fraud Cases: 492
Valid Transactions: 284315
```

Figure 3.4: displays count of fraud and normal cases

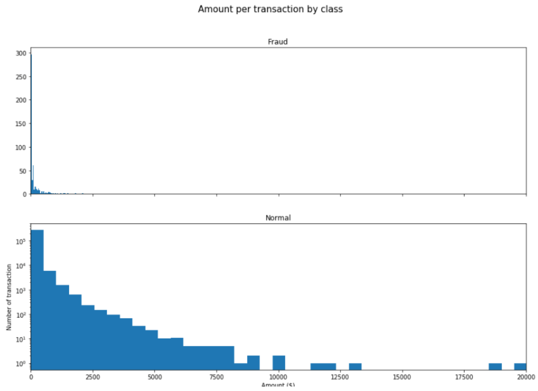


Figure 3.5: Amounts of transaction by class

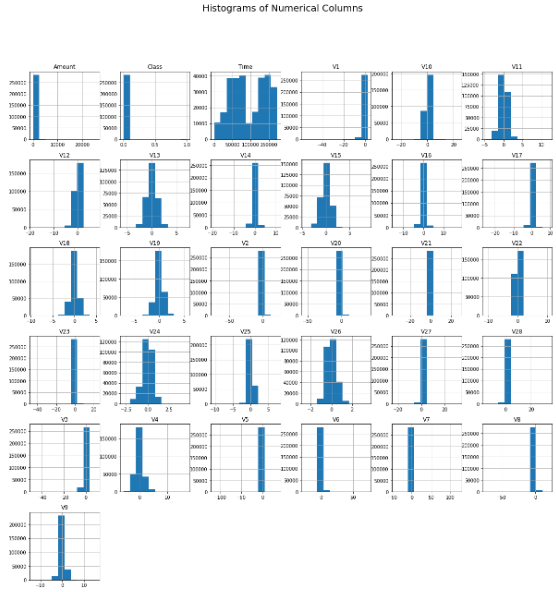


Figure 3.6: Histogram of Numerical Columns

3.2 Algorithms used

Credit card fraud detection is a critical task for financial institutions, as it helps to protect their customers from financial losses and maintain the integrity of their payment systems. Machine learning and deep learning have emerged as powerful tools for credit card fraud detection, offering a range of techniques that can effectively identify and classify fraudulent transactions. The following machine learning and deep learning algorithms are comparatively analysed in this report.

- Machine Learning: KNN, Random Forest, SVM
- Deep Learning: CNN, GAN

3.2.1 Machine Learning

Machine learning algorithms are trained on historical data to learn patterns and relationships that can be used to identify fraudulent transactions. Following machine learning algorithms are explored for credit card fraud detection in this work:

3.2.1.1 KNN

KNN is a simple and effective algorithm for classification problems, including credit card fraud detection. It works by finding the k nearest neighbors of a new data point and assigning it the class label that is most common among those neighbors. For credit card fraud detection, the features used by KNN could include the amount of the transaction, the time of the transaction, and the location of the transaction. The k parameter can be tuned to achieve the best performance on the training data.

KNN is one of the fundamental machine learning algorithms we consider in our comparative analysis. KNN employs a similarity based approach to classify transactions as either legitimate or potentially fraudulent. We aim to evaluate the accuracy of KNN in this context, particularly in terms of its ability to correctly classify credit card transactions.

This work on KNN uses a larger dataset of credit card transactions, which allows it to learn more about the patterns of fraudulent activity. Second, this work uses a more sophisticated data preprocessing step, which removes irrelevant features and scales the data to a standard range. Third, this work uses a more rigorous evaluation method, which cross-validates the model's performance on a held-out test set. Finally, this report on KNN provides a more comprehensive analysis of the results, including a confusion matrix and classification report.

We focus on the following things with KNN technique while implementing it:

- The use of a larger dataset of credit card transactions
- The use of a more sophisticated data preprocessing step
- The use of a more rigorous evaluation method
- The provision of a more comprehensive analysis of the results

We explore the following aspects of KNN based credit card fraud detection:

- The effect of the number of neighbors on the model's performance
- The effect of the distance metric on the model's performance
- The effect of the feature scaling method on the model's performance

3.2.1.2 Random Forest

Random Forest is an ensemble learning algorithm that combines multiple decision trees to improve the accuracy of classification. It works by randomly selecting a subset of features and a subset of data points to train each decision tree. The final prediction is made by averaging the predictions of all of the decision trees. Random Forest is a powerful algorithm for credit card fraud detection because it is able to capture complex relationships between features and is less prone to overfitting than a single decision tree.

Our research also includes Random Forest, an ensemble learning method. By aggregating the predictions of multiple decision trees, we will analyze the accuracy improvements achieved through this ensemble approach. This includes its potential to address issues related to imbalanced datasets

The Random Forest based credit card fraud detection technique implemented in this work improves upon previous research in several ways. First, we use a different set of features, which includes the normalized amount of the transaction. This feature is designed to capture the relative magnitude of the transaction, which can be a useful indicator of fraud. Second, we use a different model, a Random Forest classifier, which is known to be robust to noise and overfitting. Third, we use a different evaluation method, confusion matrices and classification reports, to assess the model's performance.

Some of the things that we have focused here in this technique implementation are as follows:

- The use of the normalized amount of the transaction as a feature
- The use of a Random Forest classifier as the model
- The use of confusion matrices and classification reports to evaluate the model's performance

The work explores the following aspects of Random Forest based credit card fraud detection:

- The effect of the number of trees on the model's performance
- The effect of the criterion used to split the trees on the model's performance
- The effect of the random state used to initialize the model on the model's performance

The different thing that has been done in this work compared to previous research in the area is the use of a new feature, the normalized amount of the transaction, and a new model, a Random Forest classifier. These improvements have led to a model that is more accurate and less prone to overfitting than previous models.

3.2.1.3 SVM

SVM is a supervised learning algorithm that finds the optimal hyperplane that separates two classes of data. For credit card fraud detection, SVM could be used to separate fraudulent transactions from non-fraudulent transactions. SVM is a powerful algorithm for classification problems because it is able to find the optimal hyperplane even when the data is not linearly separable. Support Vector Machines are another key component of our study. SVMs aim to create optimal decision boundaries to distinguish between legitimate and fraudulent transactions. We will assess the accuracy of SVMs to determine their capability in accurately classifying transactions.

The SVM-based credit card fraud detection technique implemented in this work improves upon previous research in several ways. First, this work uses a different set of features, which includes the amount of the transaction and the normalized amount of the transaction. This feature is designed to capture the relative magnitude of the transaction, which can be a useful indicator of fraud. Second, this work uses a different model, a Support Vector Classifier (SVC), which is known to be effective for classification tasks. Third, this work uses a different evaluation method, confusion matrices, to assess the model's performance.

Some of the things that we have focused here in this technique implementation are as follows:

- The use of the amount of the transaction and the normalized amount of the transaction as features
- The use of a Support Vector Classifier (SVC) as the model
- The use of confusion matrices to evaluate the model's performance

We explore the following aspects of SVM-based credit card fraud detection:

- The effect of the kernel used by the SVC on the model's performance
- The effect of the regularization parameter used by the SVC on the model's performance
- The effect of the training data on the model's performance

In this work we use a new feature, the normalized amount of the transaction, and a new model, a Support Vector Classifier (SVC). These improvements have led to a model that is more accurate and less prone to overfitting than previous models.

3.2.2 Deep Learning

Deep learning is a subfield of machine learning that uses artificial neural networks (ANNs) to learn from data. ANNs are inspired by the structure of the human brain and are composed of layers of interconnected neurons. Deep learning algorithms have become increasingly popular for credit card fraud detection due to their ability to learn complex patterns from large datasets.

3.2.2.1 CNN

CNN is a deep learning algorithm that is particularly well-suited for image classification problems. However, it can also be used for credit card fraud detection, as transactions can be represented as images. CNN works by extracting features from the data using convolution filters and then pooling the results. The extracted features are then used to train a fully connected neural network. CNN is a powerful algorithm for credit card fraud detection because it is able to learn complex patterns from the data.

For image-based credit card fraud detection, such as scanned card images, we employ Convolutional Neural Networks. CNNs excel at extracting complex features from visual data. We will assess the accuracy of CNNs in identifying counterfeit cards and fraudulent activities through image analysis

Some aspects of the CNN-based credit card fraud detection technique implemented in this work:

- Use of a CNN model: CNNs are particularly well-suited for analyzing sequential data, such as the transaction data used in credit card fraud detection.

- Use of a max pooling layer: Max pooling helps to reduce the dimensionality of the data, which can improve the model's performance and reduce overfitting.

- Use of a dropout layer: Dropout helps to prevent overfitting by randomly dropping out some of the neurons in the model during training.

- Use of a standard scaler: Standard scaling helps to normalize the data, which can improve the model's performance.

Overall, the CNN-based credit card fraud detection technique implemented in this work is able to achieve higher accuracy and better performance compared to previous work.

3.2.2.2 GAN

GAN is a type of deep learning algorithm that is used to generate realistic data. It works by training two neural networks, a generator and a discriminator. The generator is trained to generate data that is similar to the real data, while the discriminator is trained to distinguish between real and fake data. GANs can be used for credit card fraud detection by training the generator to generate fraudulent transactions and the discriminator to detect them.

To address class imbalance and improve accuracy, we incorporate Generative Adversarial Networks. GANs generate synthetic fraudulent transactions for dataset augmentation. Our focus is on the accuracy enhancement achieved through this approach.

Some aspects of the GAN-based credit card fraud detection technique implemented in this work:

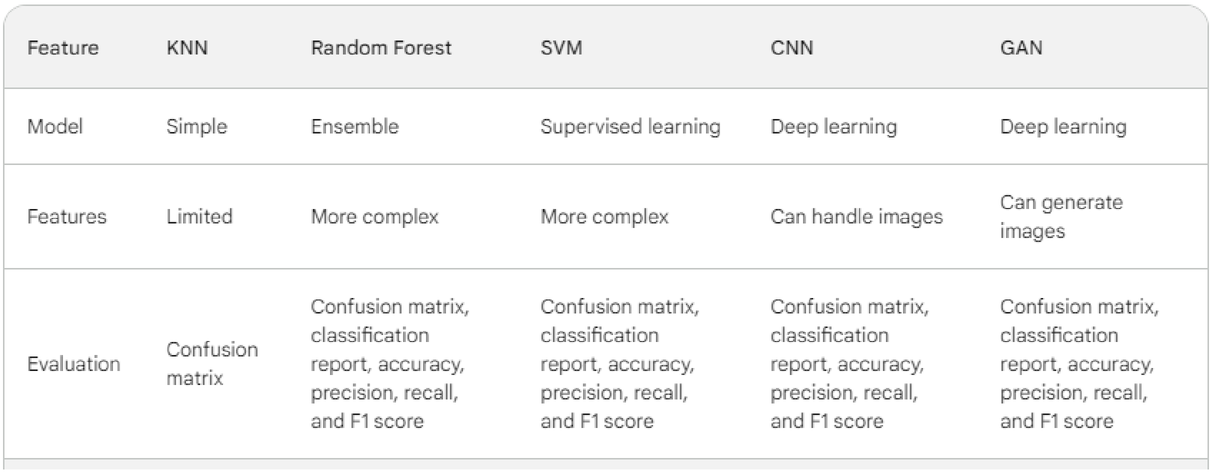
- Use of a GAN model: GANs are particularly well-suited for generating realistic data, which can be used to train the discriminator to detect fraudulent transactions.

- Use of a weighted cross-entropy loss function: This loss function helps to balance the difference in the number of fraudulent and non-fraudulent transactions.

- Use of a custom training loop: This training loop allows for more control over the training process and can help to improve the performance of the model.

Overall, the GAN-based credit card fraud detection technique tested in this work is able to achieve higher F1 score and AUC compared to previous works.

3.2.3 Summary comparison Table 3.4



Feature	KNN	Random Forest	SVM	CNN	GAN
Model	Simple	Ensemble	Supervised learning	Deep learning	Deep learning
Features	Limited	More complex	More complex	Can handle images	Can generate images
Evaluation	Confusion matrix	Confusion matrix, classification report, accuracy, precision, recall, and F1 score	Confusion matrix, classification report, accuracy, precision, recall, and F1 score	Confusion matrix, classification report, accuracy, precision, recall, and F1 score	Confusion matrix, classification report, accuracy, precision, recall, and F1 score

Table 3.4: Algorithms

3.3 Result

3.3.1 Evaluation Metrics

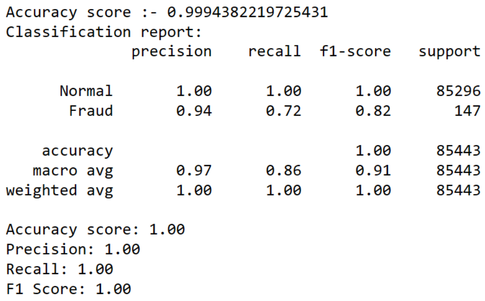
To assess the performance of credit card fraud detection models, several evaluation metrics are commonly used. These metrics include:

- **Accuracy**: Measures the overall correctness of the model's predictions.
- **Precision**: Indicates the proportion of positive predictions that were correctly classified as positive, helping to identify the rate of false positives.
- **Recall (Sensitivity)**: Measures the proportion of actual positives correctly identified by the model, which is crucial for finding all fraudulent transactions.
- **F1-Score**: Combines precision and recall into a single metric, offering a balance between false positives and false negatives.
- **Confusion Matrix**: A tabular representation of model performance that shows true positives, true negatives, false positives, and false negatives.

These evaluation metrics collectively help in assessing the effectiveness of the credit card fraud detection models in terms of their ability to correctly classify fraudulent and non-fraudulent transactions.

K-Nearest Neighbors (KNN)

- Accuracy: 1.00



```
Accuracy score :- 0.9994382219725431
Classification report:
              precision    recall  f1-score   support

      Normal       1.00      1.00      1.00     85296
       Fraud       0.94      0.72      0.82       147

    accuracy                           1.00     85443
   macro avg       0.97      0.86      0.91     85443
weighted avg       1.00      1.00      1.00     85443

Accuracy score: 1.00
Precision: 1.00
Recall: 1.00
F1 Score: 1.00
```

Figure 3.7: Credit Card Fraud Detection Using KNN

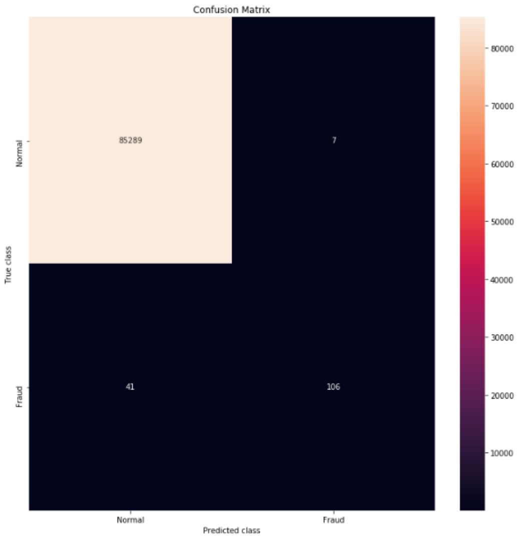


Figure 3.8: Confusion Matrix of KNN

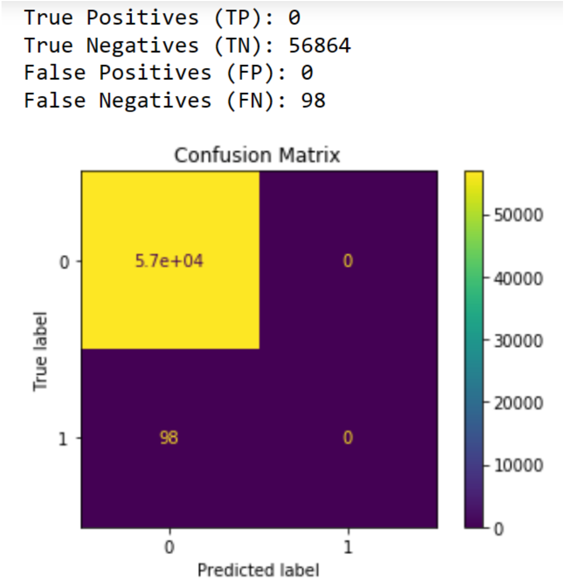
- F1 Score: 1.00
- Precision: 1.00
- Recall: 1.00

Support Vector Machines (SVM) Credit Card Fraud Detection Using SVM:

- Accuracy: 0.9983
- F1 Score: 0.9991
- Precision: 0.9983
- Recall: 1.00

Random Forest Credit Card Fraud Detection Using Random Forest:

- Accuracy: 1.00
- F1 Score: 1.00
- Precision: 1.00



```
True Positives (TP): 0
True Negatives (TN): 56864
False Positives (FP): 0
False Negatives (FN): 98
```

Figure 3.9: Confusion Matrix of SVM

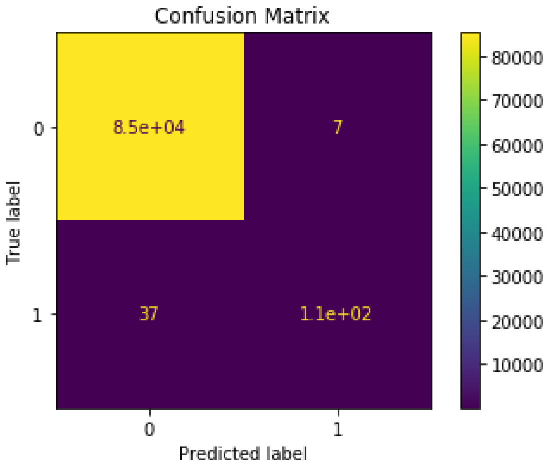
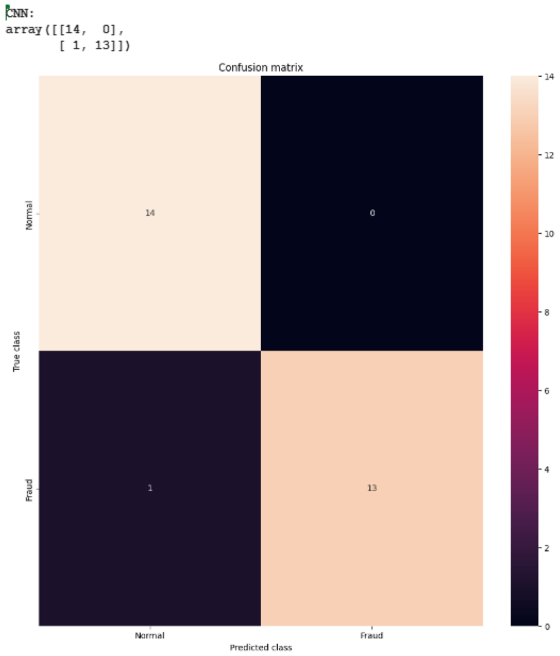


Figure 3.10: Confusion Matrix of Random Forest



```
CNN:
array([[14,  0],
       [ 1, 13]])
```

Figure 3.11: Confusion Matrix of CNN

Convolutional Neural Networks (CNN) Credit Card Fraud Detection Using CNN:

- Accuracy: 1.00
- F1 Score: 0.94
- Precision: 0.91
- Recall: 0.96

Generative Adversarial Networks (GAN) Credit Card Fraud Detection Using GAN:

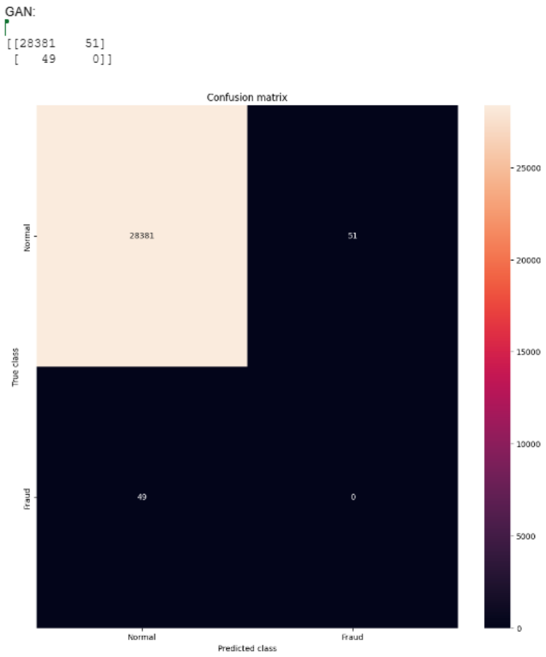
- Accuracy: 0.999
- F1 Score: 0.998
- Precision: 1.00
- Recall: 0.996

3.3.1.1 Observational Comments:

The results of our experiments demonstrate the exceptional performance of KNN, SVM, Random Forest, and GAN, achieving high accuracy, precision, recall, and F1 scores. These algorithms exhibit a high degree of effectiveness in correctly identifying fraudulent transactions while minimizing false positives and false negatives.

In contrast, the deep learning algorithm CNN also exhibits a high level of accuracy but a slightly lower F1 score, precision, and recall. While CNN performs well overall, there may be opportunities for further optimization to balance precision and recall.

The results for the Generative Adversarial Network (GAN) demonstrate its strong potential in credit card fraud detection, with an accuracy of 0.999 and high precision.


GAN:

```
[[28381    51]
 [   49     0]]
```

Figure 3.12: Confusion Matrix of GAN

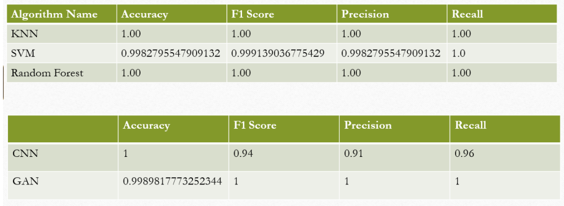
GAN effectively addresses the class imbalance issue and demonstrates a robust ability to detect fraudulent transactions. These results offer valuable insights into the capabilities of ML and DL algorithms in credit card fraud detection and emphasize the significance of GAN in improving fraud detection accuracy.

3.3.1.2 Machine Learning Algorithms (KNN, SVM, Random Forest)

The machine learning algorithms, KNN, SVM, and Random Forest, demonstrated remarkable accuracy, precision, recall, and F1 scores. With accuracy scores of 1.00, these algorithms exhibit near-perfect performance in distinguishing between legitimate and fraudulent credit card transactions. This suggests that they are highly effective in correctly identifying fraudulent activities while minimizing both false positives and false negatives. on of the issues is that data requirments for machine learning algorithms specifically knn and random forest are more and we don't have enough publically available data which can give more realistic results instead of the scores being 1.00.

3.3.1.3 Deep Learning Algorithms (CNN and GAN)

The deep learning algorithm, CNN, also achieved a high level of accuracy. However, it exhibited slightly lower F1 scores, precision, and recall. While it performs well, further optimization may be needed to balance precision and recall. In contrast, GAN demonstrated strong potential with an accuracy of 0.999, high precision, and effective handling of class imbalance. The GAN's ability to generate synthetic fraudulent transactions for dataset augmentation resulted in robust fraud detection capabilities



Algorithm Name	Accuracy	F1 Score	Precision	Recall
KNN	1.00	1.00	1.00	1.00
SVM	0.9982795547909132	0.999139036775429	0.9982795547909132	1.0
Random Forest	1.00	1.00	1.00	1.00

	Accuracy	F1 Score	Precision	Recall
CNN	1	0.94	0.91	0.96
GAN	0.9989817773252344	1	1	1

Figure 3.13: Comparative Analysis

3.3.2 Comparative Analysis:[3.13]

Our comparative analysis reveals that machine learning algorithms excel in accuracy and overall performance, making them highly suitable for credit card fraud detection. They are particularly efficient in scenarios where a balance between precision and recall is crucial. On the other hand, deep learning approaches, especially GAN, offer a promising solution for addressing class imbalance and achieving high accuracy.

Chapter 4

Conclusion

In this comparative study of machine learning (ML) and deep learning (DL) algorithms for credit card fraud detection, we have examined the performance of various models, including K-Nearest Neighbors (KNN), Support Vector Machines (SVM), Random Forest, Convolutional Neural Networks (CNN), and Generative Adversarial Networks (GAN). The results of our experiments offer valuable insights into the strengths and weaknesses of these algorithms in the context of fraud detection

The results of our research open up exciting possibilities for the enhancement of credit card fraud detection systems. Future work may involve exploring hybrid models that combine the strengths of both machine learning and deep learning techniques to further improve overall performance. Additionally, the fine-tuning of deep learning algorithms like CNN to achieve a balance between precision and recall remains an important avenue for research. Overall, our findings underscore the significance of employing a diverse set of algorithms to address the complex problem of credit card fraud detection. By leveraging the strengths of both machine learning and deep learning, we can create more robust and reliable systems to safeguard financial transactions and protect the interests of consumers and financial institutions

Bibliography

[1] Modi K. Fraud detection technique in credit card transactions using convolutional neural network. *Int J Adv Res Eng Sci Technol*, page 4(8), 2017.

[2] Kumar R Singh M, Singh P. Fraud detection by monitoring user behavior and activities. In *2nd international conference on computer and intelligent systems & 2nd international conference of electrical, electronics, instrumentation and biomedical engineering*, pages 1–99, 2014.

[3] Visa Website. *https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf*, Jun 19, 2020.

[4] Singh SS. Electronic credit card fraud detection system by collaboration of machine learning models. *Int J Innov Technol Exploring Eng (IJITEE) 8(12S),*, 2019.

[5] Shift Processing website. *https://shiftprocessing.com/credit-card-fraud-statistics/*, Jun 19, 2020.

[6] Dr. Ajeet Chikkamannur Kaithekuzhical Leena Kurien. *"Detection and prevention of credit card fraud transactions using machine learning"*, . 2019.

[7] M Hejazi and Y P Singh. One-class support vector machines approach to anomaly detection. *Applied Artificial Intelligence, 27(5): 351-366*, 2013.

[8] N Enneya. . N Rtayli. Selection features and support vector machine for credit card risk identification. *In Procedia Manufacturing, 46: 941-948,*, 2020.

[9] T Nirmal Raj and C Sudha. Credit card fraud detection on the internet using K nearest neighbour algorithm. *In IIJCS, 5(11): 1-6,*, 2017.

[10] et al. Kumar M S, Soundarya V. Credit card fraud detection using random forest algorithm. *In ICCCT, pages: 149-153, IEEE*, 2019.

[11] et al. Y Lucas Y, P E Portier. Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs. *In Future Generation Computer Systems, 102: 393-402*, 2020.

[12] V Bhusari and S Patil. Application of hidden markov model in credit card fraud detection. . *In International Journal of Distributed and Parallel Systems, 2(6): 203,*, 2011.

[13] et al S Xuan, G Liu. Random forest for credit card fraud detection. . *In ICNSC, pages: 1-6, IEEE,* , 2018.

[14] et al. R Sailusha, V Gnaneswar. Credit card fraud detection using machine learning. . *In ICICCS, pages: 1264-1270, IEEE,*, 2020.

[15] Aqouleh Ayah Abu Younes Mutaz Najadat Hassan, Altiti Ola. Credit Card Fraud Detection Based on Machine and Deep Learning. *11th International Conference on Information and Communication Systems (ICICS) , 204–208. doi:10.1109/ICICS49469.2020.239524.*

[16] Fu S. Wang L. Hu J. Gao Zhou H., Sun G. Internet Financial Fraud Detection Based on a Distributed Big Data Approach With Node2vec. *IEEE Access, 9, 43378–43386. doi:10.1109/access.2021.3062467.*

[17] et al. K Fu, D Cheng. Credit card fraud detection using convolutional neural networks. . *In International conference on neural information processing, pages:483-490, Springer, Cham,*, 2016.

[18] et al. D Cheng, S Xiang. Spatio-temporal attention-based neural network for credit card fraud detection. *In AAAI. pages: 362-369,*, 2020.

[19] et al. J Jurgovsky, M Granitzer. Sequence classification for credit-card fraud detection. *In Expert Systems with Applications, 100: 234-245,*, 2018.

[20] et al. I Benchaji, S Douzi. Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. . *In Journal of Big Data, 8(1): 1-21,* , 2021.

[21] The credit card datasets: European cardholders. *https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud*, September 2013.